Bugzilla ID: 536318
Bugzilla Summary: EV enable VeriSign SHA256 root certificate

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	Data
CA Name	Symantec VeriSign Authentication Services
Website URL	http://www.symantec.com http://www.verisign.com
Organizational type	Commercial
Primary market / customer base	Symantec acquired the VeriSign Authentication Services and root certificates, and is a major commercial CA with worldwide operations and customer base.
CA Contact Information	CA Email Alias: practices@symantec.com CA Phone Number: 1 650.961.7500 Title / Department: The Certificate Policy Manager

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

	SHA 256 Root
Cert Name	VeriSign Universal Root Certification Authority
Description	This SHA256 root is currently included in NSS. Inclusion bug #484901. This request is to enable EV. This root is currently used to sign the VeriSign Class 3 SSP Intermediate CA - G2, which is used to issue Non-Federal SSP SHA256 CAs to customers, but those SubCAs are operated internally by Symantec. This root will be used in the future to sign certificates for SSL-enabled servers, and may be used to sign certificates for digitally-signed executable code objects.
Root cert URL	https://bugzilla.mozilla.org/attachment.cgi?id=368998
SHA-1 fingerprint	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54
Valid from	2008-04-01
Valid to	2037-12-01
Cert Version	3
Modulus length	2048
Cert Signature Algorithm	Sha256RSA
Enabled Trust Bits	Websites Email Code Signing
Test URL	https://ssltest26.bbtest.net/ (Note: EV intermediate issuing CA is not yet created)
CRL URL	http://crl.verisign.com/universal-root.crl
CRL update frequency	CPS section 4.9.7, CRL Issuance Frequency**:** CRLs for end-user Subscriber Certificates are issued at least once per day.

	Symantec: CRLs are issued at least once per day (they are actually issued more often than that). They have a validity period of 2 weeks. CPS Appendix B1, Section 26: For EV Certificates: (A) CRLs are be updated and reissued at least every seven (7) days, and the nextUpdate field value SHALL NOT be more than ten (10) days; or (B) Symantec's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days
OCSP Responder	Ready and in place at ocsp.verisign.com (other domain names are used and CNAMEd to ocsp.verisign.com). CPS Appendix B1, For EV Certificates: Symantec's Online Certificate Status Protocol (OCSP) is updated at least every four (4) days, and with a maximum expiration time of ten (10) days
Verification Type	OV, EV
EV policy OID	2.16.840.1.113733.1.7.23.6
Hierarchy	A Class 3 intermediate CA will be created under this root for EV issuance. This root is currently used to sign the VeriSign Class 3 SSP Intermediate CA - G2, which is used to issue Non-Federal SSP SHA256 CAs to customers, but those SubCAs are operated internally by Symantec.
Externally Operated SubCAs	None, and none planned.
Cross-Signing	This root has signed an intermediate called "VeriSign Class 3 SSP Intermediate CA - G2", which is cross-signed with FBCA.
CP/CPS	CA Hierarchy Diagram: http://www.verisign.com/repository/hierarchy/hierarchy.pdf CPS: http://www.verisign.com/repository/CPS/ CP: http://www.verisign.com/repository/vtnCp.html Symantec doesn't list all of their roots in the CPS. They refer to the PCAs generally.
AUDIT	Audit Type: WebTrust for CA and WebTrust EV Auditor: KPMG, http://www.kpmg.com/ Audit Report & Management Assertions: https://cert.webtrust.org/SealFile?seal=304&file=pdf (2010.11.30) This document contains three audit reports and the corresponding management assertions.
Organization Identity Verification	CPS Table 2: Only Class 3 and Class 3 EV Certificates can be used for SSL/TLS. CPS Section 1.4.1: High assurance certificates are individual and organizational Class 3 Certificates that provide a high level of assurance of the identity of the Subscriber in comparison with Class 1 and 2. High assurance with extended validation certificates are Class 3 certificates issued by Symantec in conformance with the Guidelines for Extended Validation Certificates. CPS Section 3.2.2, Authentication of Organization identity, provides the details for verifying the identity of the certificate subscriber.
Domain Name Ownership / Control	CPS Section 1.4.1: According to tables 1 and 2, only Class 3 certificates issued to organizations can be used for SSL and Code Signing. Therefore all SSL certs are of OV verification type. CPS Section 1.4.1.2, Certificates issued to Organizations: Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non-verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain.

	CPS Section 3.2.2: Where a domain name or e-mail address is included in the certificate Symantec authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain.
EV Validation	CPS Appendix B1, Section 3, EV Certificate Warranties and Representations Right to Use Domain Name: Symantec has taken all steps reasonably necessary in terms of the Guidelines to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate owns or has the exclusive right to use the domain name(s) listed in the EV Certificate; CPS Appendix B1 Section*18,* Verification of Applicant's Domain Name Symantec verifies Applicant's registration of the domain name(s) to be listed in the EV Certificate, satisfy the following requirements: (1) The domain name is registered with an Internet Corporation for Assigned Names and Numbers (ICANN)-approved registrar or a registry listed by the Internet Assigned Numbers Authority (IANA); (2) Domain registration information in the WHOIS database SHOULD be public and SHOULD show the name, physical address, and administrative contact information for the organization. For Government Entity Applicants, the Symantec MAY rely on the domain name listed for that entity in the records of the QGIS in Applicant's Jurisdiction to verify Domain Name. (3) The Applicant is the registered holder of the domain name or has been granted the exclusive right to use the domain name by the registered holder of the domain name (4) The Applicant is aware of its registration or exclusive control of the domain name; Symantec performs a WHOIS inquiry on the Internet for the domain name supplied by the Applicant, to verify that the Applicant is the entity to whom the domain name is registered. Where the WHOIS record indicates otherwise, Symantec will require the WHOIS record to be updated to reflect the Applicant as the registered holder of the domain. Confirmation that the registered owner of the domain name is a Parent/Subsidiary Company of Applicant, or a registered trading name of Applicant is sufficient to establish that Applicant is the registered owner of the domain name. In cases where Applicant is not the registered holder of the domain name, or domain registration information cannot be obtained from WHOIS, Symantec may obtain positive confirmation from the registered domain holder that the applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name (FQDN). In these circumstances, Symantec also verifies the Applicant's exclusive right to use the domain name using one of the following methods: (A) Relying on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; or (B) Relying on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, that it controls the confirmed domain name. In cases where the registered domain holder cannot be contacted, Symantec shall: Rely on a Verified Legal Opinion to the effect that the Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet, *and*

	o Rely on a representation from the Contract Signer, or the Certificate Approver if expressly authorized in a mutually agreed upon contract, coupled with a practical demonstration by the Applicant establishing that it controls the confirmed domain name. by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing the Applicant's FQDN; Symantec may verify the Applicant is aware that it has exclusive control and/or ownership of the domain name by obtaining a Confirmation from Corporate Contact verifying that the Applicant is aware that it has exclusive control of the domain name.
Email Address Ownership / Control	Email certs can be issued for Class 1, 2, and 3 verification levels, for both individuals and organizations. The absolute minimum verification is for Class 1 individual. CPS section 3.2.3, Class 1: No identity authentication. There is a limited confirmation of the Subscriber's e-mail address by requiring the Subscriber to be able to answer an e-mail to that address. CPS section 3.2.3, Class 2 individual: Authenticate identity by matching the identity provided by the Subscriber to: information residing in the database of a Symantec-approved identity proofing service, such as a major credit bureau or other reliable source of information providing, or information contained in the business records or databases of business information (employee or customer directories) of an RA approving certificates to its own affiliated individuals
Identity of Code Signing Subscriber	CPS Section 1.4.1: According to table 2, only Class 3 (High Assurance) certificates can be used for Code Signing.

Potentially Problematic Practices	http://wiki.mozilla.org/CA:Problematic_Practices
	• 1.1 Long-lived DV certificates
	  ○ SSL certs are OV/EV
	  ○ CPS section 6.3.2: Certificates issued by CAs to end-user Subscribers may have Operational Periods longer than two years, up to six years, if the following requirements are met … Subscribers are required to undergo re-authentication at least every 3 years under Section 3.2.3.
	  ○ From Symantec: This policy will be modified to comply with the CA/Browser Forum's Base Requirements by 1 July, 2012.
	• 1.2 Wildcard DV SSL certificates
	  ○ SSL certs are OV/EV
	  ○ The only mention of wildcard certs in the CPS is to state that wildcard certificates are not allowed for EV certificates.
	• 1.3 Email Address Prefixes for DV Certs
	  ○ SSL certs are OV/EV
	• 1.4 Delegation of Domain / Email validation to third parties
	  ○ From Audit: "For the VeriSign/RSA Secure Server CA, VeriSign International Server CA – Class 3, VeriSign Class 3 Secure Server CA, VeriSign Class 3 Secure Server CA – G2, and VeriSign Class 3 Public Primary Certification Authority – G5, Symantec makes use of external registration authorities for specific subscriber registration activities as disclosed in the VTN CPS on Symantec's VeriSign website. Our examination did not extend to the controls of external registration authorities."
	• 1.5 Issuing end entity certificates directly from roots
	  ○ Roots are offline, and only sign intermediate certificates.
	• 1.6 Allowing external entities to operate subordinate CAs

	○ No externally-operated subCAs are planned to be issued under this root. • 1.7 Distributing generated private keys in PKCS#12 files ○ CPS Section 3.2.1, Method to Prove Possession of Private Key: The certificate applicant must demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate. The method to prove possession of a private key shall be PKCS #10, another cryptographically equivalent demonstration, or another Symantec-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pregenerated keys are placed on smart cards. • 1.8 Certificates referencing hostnames or private IP addresses ○ Non EV certificates may contain host names after verification with the organization. IP addresses verified to be within the private range may be refenced in Standard Intranet and Premium Intranet Certificates. ○ CPS section 3.2.2, Table 6: Symantec verifies that the host name or IP address assigned to a Device is not accessible from the Internet (publicly facing), and is owned by the Certificate Subscriber. • 1.9 Issuing SSL Certificates for Internal Domains ○ Non EV certificates may contain internal domains. • 1.10 OCSP Responses signed by a certificate under a different root ○ Not applicable • 1.11 CRL with critical CIDP Extension ○ Not applicable • 1.12 Generic names for CAs ○ CA names include VeriSign